# Bitcoin

## Crittografia

Luciano Margara

Unibo

2022

# Valore

# Simbolo

# Introduzione

Bitcoin (in acronimo BTC, indicato in simbolo come una B attraversata da due barre verticali) indica una unità monetaria nata in un articolo pubblicato nel 2008 da Satoshi Nakamoto, un misterioso autore giapponese la cui identità è ignota tanto da indurre molti a credere che dietro al nome si celi un gruppo di ricercatori

# Introduzione

Il primo programma per la sua gestione, chiamato Bitcoin-Qt, fu distribuito dallo stesso autore nel 2009 come codice open source, per essere poi aggiornato e ormai sostituito dalla nuova versione Bitcoin Core. Il software consente scambi finanziari sulla rete ma contribuisce anche a creare bitcoin in un sistema completamente decentralizzato che segue un classico approccio dei sistemi Peer-to-Peer (P2P) ove la correttezza delle transazioni può essere controllata da tutti gli utenti sia in tempo reale che in qualsiasi momento successivo

# Impatto psicologico

L’intero sistema è quindi soggetto solo al controllo degli utenti. Basta questa caratteristica a far comprendere il grande impatto psicologico del metodo

# Indirizzo

Consiste in un identificatore dei singoli utenti sulla rete.

Non è quindi un indirizzo in senso classico né un indirizzo IP

# Portafogli (wallet)

Insieme di credenziali digitali che attesta la proprietà in bitcoin di un utente

# Transazione

Scambio di bitcoin tra due utenti

# Broadcast

Indica una comunicazione in rete diretta a tutti gli utenti

# Libro contabile (ledger)

Cuore del sistema che contiene la registrazione pubblica di tutte le transazioni eseguite nella storia di bitcoin

# Blocco e block-chain

Blocco di transazioni e catena di blocchi.

Catena di blocchi = libro contabile

# Mining

## Operazioni per il mantenimento della catena di blocchi

Il mining (o estrazione) in Bitcoin è il processo mediante il quale nuovi bitcoin vengono messi in circolazione e le transazioni vengono verificate e aggiunte al registro pubblico (blockchain). In pratica, una rete decentralizzata di computer (i “miner”) compete per risolvere complessi problemi crittografici basati sull’algoritmo SHA-256: chi per primo trova la soluzione valida ottiene il diritto di creare un nuovo blocco e ricevere in premio una quantità prefissata di bitcoin.

Tecnicamente, il mining utilizza un meccanismo di Proof of Work: i miner devono calcolare ripetutamente l’hash di un blocco variando un parametro (nonce) finché l’hash risultante non rispetta un criterio di difficoltà (numero di zeri iniziali). Questa difficoltà viene aggiustata automaticamente ogni 2.016 blocchi (circa ogni due settimane) per mantenere il tempo di creazione di ogni blocco intorno ai 10 minuti. Per affrontare i crescenti requisiti computazionali, i miner si organizzano spesso in pool di mining, aggregando la potenza di calcolo per ottenere ricompense in modo più stabile e proporzionale al contributo di ciascun partecipante.

# Procedura secondo Nakamoto

1. Le nuove transazioni sono diffuse sulla rete via broadcast
2. Ogni nodo del sistema raccoglie le nuove transazioni in un blocco
3. Ogni nodo cerca di individuare una dimostrazione di correttezza per il suo blocco. Questo volutamente implica la soluzione di un problema difficile
4. Quando un nodo trova una dimostrazione di correttezza la diffonde per broadcast a tutti i nodi per inserire il blocco nel block-chain. Un premio in bitcoin viene accreditato al nodo autore della dimostrazione

# Procedura secondo Nakamoto

5. I nodi accettano il blocco solo se le transazioni in esso conutente sono valide e non sono apparse in blocchi precedenti
6. I nodi esprimono la loro accettazione del blocco iniziando a creare un nuovo blocco da inserire nel block-chain

# Chiavi

Il software cliente di bitcoin, attualmente Bitcoin Core, è caricato sul PC o sullo smartphone di ogni utente $A$ e genera anzitutto una coppia di chiavi privata-pubblica $k_A[prv], k_A[pub]$ per un cifrario asimmetrico su curve ellittiche

# Curva Ellittica per Blockchain

Curva: $secp256k1$

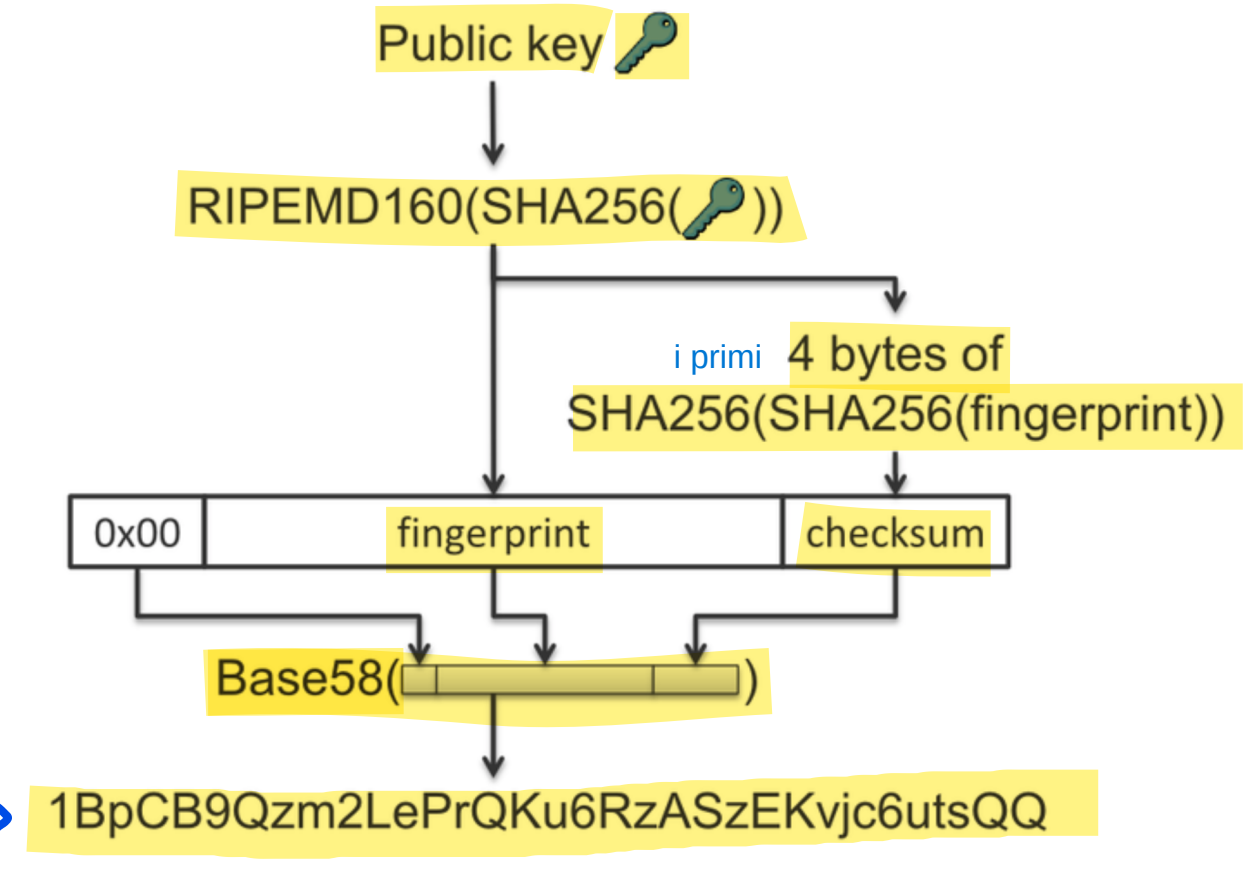
$y^2 = x^3 + 7$

$p = 115792089237316195423570985008687907853269984665640564039457584007908834671663$

# Indirizzo

La chiave privata $k_A[prv]$ è ovviamente nota solo ad $A$ che la usa per firmare le transazioni che genera e diffonde sulla rete. La chiave pubblica $k_A[pub]$ è utilizzata per controllare la firma di $A$ ed è anche impiegata come suo identificatore: a tale scopo viene trasformata attraverso applicazioni ripetute della funzione hash SHA-256 (immagine a 256 bit), per essere poi compressa via RIPEMD-160 in un'immagine di 160 bit in testa alla quale è aggiunta una speciale sequenza che indica che la stringa complessiva è di fatto un indirizzo bitcoin

# Indirizzo


Public key
RIPEMD160(SHA256( ))
i primi 4 bytes of
SHA256(SHA256(fingerprint))
0x00
fingerprint
checksum
Base58( )
1BpCB9Qzm2LePrQKu6RzASzEKvjc6utsQQ

# Base58

Base58 è un insieme di schemi di codifica da binario a testo, specificati da Satoshi Nakamoto per la rete Bitcoin, al fine di rappresentare numeri interi grandi come testo alfanumerico. Da allora, è stato applicato ad altre crittovalute e applicazioni. È simile al Base64, ma è stato modificato per eliminare sia i caratteri non alfanumerici che quelle lettere che potrebbero essere confuse con altre, quando stampate. È quindi progettato per gli utenti umani che inseriscono manualmente i dati, copiandoli da una qualche sorgente visiva, ma consente anche una facile copia e incolla, perché un doppio clic di solito seleziona l'intera stringa.

# Base58

Rispetto al Base64, sono state eliminate le seguenti lettere tra loro simili e in grado generare errati riconoscimenti: 0 (zero) e O ("o" maiuscola), così come I ("i" maiuscola) e l (lettere L minuscola), oltre ai caratteri non alfanumerici + (più) e / (slash).

# Le transazioni bitcoin

Come già osservato questo indirizzo non corrisponde a una locazione del cliente ma a un modo per identificarlo, sia per potergli dirigere una transazione che per controllare che possieda effettivamente i fondi che pretende di spendere

# Le transazioni bitcoin

Una transazione in bitcoin ha la forma:
Il pagatore $A$ vuole inviare $X$ bitcoin al ricevente $B$
completata dalla firma digitale di $A$
Si noti che $A$ e $B$ sono indicati attraverso i loro indirizzi bitcoin e la transazione viene inviata per broadcast a tutti gli utenti

# Le transazioni bitcoin

Diversamente da ogni altra forma di transazione economica, il ricevente $B$ non ha la garanzia che la transazione sia valida finché essa non è convalidata dalla rete. In effetti $B$ sarebbe in grado di verificare sia la firma di $A$ che i fondi che $A$ ha a disposizione, poiché la chiave pubblica di $A$ è nota e tutte le transazioni eseguite sulla rete sono pubbliche, ma non ha il tempo di verificare che $A$ non abbia utilizzato gli stessi fondi in istanti immediatamente precedenti per pagamenti diversi

# Le transazioni bitcoin

Questo sistema di verifica pubblica costituisce il vero cuore del sistema bitcoin. Si noti la differenza con il pagamento con carta di credito su Internet in cui la transazione è inviata alla banca che ha emesso la carta che ha il compito di convalidarla e di bloccare diverse richieste in successione quando i fondi concessi al cliente si esauriscono: per tale meccanismo è necessario l'intervento di un ente terzo e al di sopra agli altri (la banca), cosa che il sistema bitcoin per principio vuole evitare: anche perché, come è ovvio, quell'ente offre i suoi servizi tutt'altro che gratis

# Protocollo di transazione bitcoin

- **Messaggio:** l'utente $A$ genera un messaggio $m = adr_A - X - adr_B$, ove $adr_A$, $adr_B$ sono gli indirizzi bitcoin di $A$ e $B$, e $X$ è la somma da trasferire da $A$ a $B$.
- **Firma:** l'utente $A$ calcola l'hash $h = \text{SHA-256}(m)$ del messaggio e genera la firma $f = D(h, k_A[prv])$ per $m$
- **Broadcast:** la coppia $\langle m, f \rangle$ viene diffusa da $A$ sulla rete

# Le transazioni bitcoin

La verifica di validità della transazione è eseguita dalla rete che aggiorna in conseguenza il libro contabile. L'utente $B$ attende che la rete convalidi la transazione prima di accettarla. Tipicamente se $B$ deve spedire della merce ad $A$ in seguito al pagamento di $X$ bitcoin, e non ha motivo particolare per fidarsi di $A$, dovrà per prudenza attendere la convalida del messaggio prima della spedizione. Nel funzionamento attuale del sistema una convalida richiede qualche minuto

# Le transazioni bitcoin

La chiave privata è l'unico documento valido per dimostrare la proprietà in bitcoin di un utente $A$. La perdita della chiave comporta la perdita della proprietà a causa dell'impossibilità di firmare transazioni, e il furto della chiave da parte di un truffatore che la usi per firmare al posto di $A$ comporta anch'esso la perdita di proprietà: in entrambi i casi non vi è alcuna possibilità di recupero. La chiave privata deve quindi essere conservata con assoluta sicurezza

# Chiavi

Single Wallet | Paper Wallet | Bulk Wallet | Brain Wallet

Vanity Wallet | Split Wallet | Wallet Details

Genera un Nuovo Indirizzo | Stampa

**Indirizzo Bitcoin:**

**SHARE**

1BvmEkUT11kSpzCY2bk7xXvrB1mcxrY4CK

**Chiave privata (Wallet Import Format):**

**SECRET**

5Jmp2WH7TozUJ5riYwNkNsPBXWi8d5zaqP5wu9fmHLQEgSAKcnw

# Validazione tramite mining

Secondo Nakamoto ogni nodo del sistema bitcoin può partecipare al processo di validazione delle transazioni lanciate sulla rete.
Poiché però tale processo richiede la soluzione enumerativa di un problema esponenziale secondo un esponente $t$ che viene incrementato nel tempo, solo nodi con grande potenza di calcolo hanno la possibilità pratica di partecipare al processo ricevendo un premio in bitcoin in caso di successo

# Validazione tramite mining

La grande maggioranza dei nodi si limita a lanciare le transazioni e a controllarne la validazione effettuata da altri nodi strutturati a questo proposito. Infatti mentre la dimostrazione di validazione richiede in media $2^t$ operazioni, il controllo di correttezza della dimostrazione può essere eseguito da tutti i nodi mediante un unico semplice calcolo

# Validazione tramite mining

Il libro contabile consiste in una catena di blocchi (block-chain) ciascuno dei quali contiene una sequenza di transazioni lanciate in rete in un certo intervallo di tempo. In ogni istante il blocco corrente, ancora non inserito nella catena, contiene le ultime transazioni la cui legittimazione deve essere approvata. Tutti i blocchi precedenti sono invece già stati approvati e la catena fin lì è immutabile e contiene l'intera storia di bitcoin

# Validazione tramite mining

Il procedimento di valutazione di un blocco, oltre a controllare la legittimità delle transazioni ivi contenute, ovvero che i pagatori dispongano dei fondi necessari per ogni transazione, è associato a un'operazione detta mining.
Il mining è l'operazione con la quale si "scovano" sequenze binarie dette nonce.
Le sequenze nonce hanno particolari proprietà in relazione a tutta la sequenza di transazioni passate

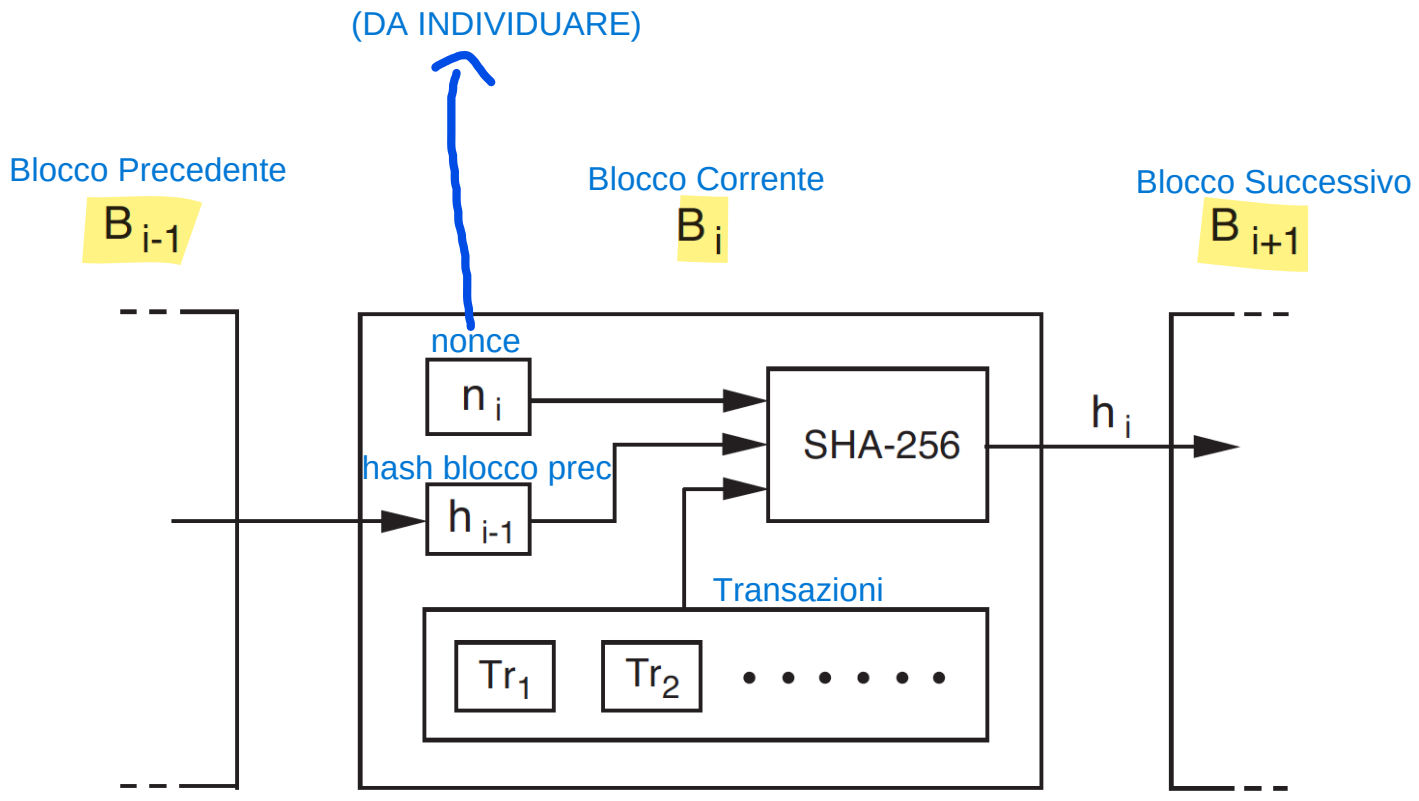
# Validazione tramite mining

Un blocco $B_i$ contiene la sequenza di transazioni relativa al suo periodo temporale, un valore hash $h_{i-1}$ proveniente dal blocco precedente e un nonce $n_i$. Il processo di mining consiste nella ricerca di un valore di $n_i$ che, concatenato alla sequenza di transizioni del blocco e ad $h_{i-1}$, generi un'immagine hash SHA-256 che inizia almeno con $t$ zeri, ove $t$ è un valore prefissato dal sistema

# Validazione tramite mining

Poiché la funzione SHA-256 è crittograficamente forte non è prevedibile in tempo polinomiale in $t$ l'immagine che genererà la presenza di un nonce arbitrario: l'unica strategia possibile è quindi enumerativa, tipicamente la prova in successione di nonce consecutivi a partire da un valore arbitrario finché se ne individua uno che genera nell'hash una sequenza iniziale di $t$ zeri. Ciò richiede in media l'applicazione di SHA-256 per $2^t$ volte mentre, ottenuto un nonce giusto, la verifica della sua proprietà richiede solo un calcolo della funzione hash

# Block-chain


(DA INDIVIDUARE)
Blocco Precedente
B i-1
Blocco Corrente
B i
Blocco Successivo
B i+1
nonce
n i
hash blocco prec
h i-1
SHA-256
h i
Transazioni
Tr1
Tr2

# Validazione tramite mining

Quando un nodo di mining $N$ trova un valore giusto di nonce convalida il blocco trasmettendolo a tutti gli altri nodi. Questi controllano a loro volta le transizioni ivi contenute e il nonce indicato da $N$ e confermano sulla rete la loro accettazione del blocco che viene così inserito nel block-chain e non è più alterabile

# Validazione tramite mining

In presenza di più blocchi convalidati contemporaneamente il sistema accetta quello che contiene il maggior numero di transazioni. Il sistema è dimensionato in modo che la validazione di un blocco avvenga circa ogni dieci minuti: poiché questo tempo è legato alla scoperta di un nonce, il sistema adegua in continuazione il valore di $t$ in funzione del numero e della potenza di calcolo dei nodi di mining presumibilmente in azione. E poiché il numero di tali nodi e soprattutto la loro potenza di calcolo crescono costantemente nel tempo, il valore di $t$ viene costantemente aumentato

# Halving

L’halving di Bitcoin è un evento protocollo-definito che dimezza la ricompensa erogata ai miner per ogni blocco estratto, e si verifica ogni 210 000 blocchi (circa ogni quattro anni). Lo scopo è controllare l’inflazione di Bitcoin riducendo progressivamente la quantità di nuove monete immesse in circolazione, fino al limite massimo di 21 milioni di BTC.
Ogni halving riduce del 50 % la ricompensa in BTC per blocco (ad esempio, da 6,25 BTC a 3,125 BTC nell’halving del 2024).
Questo meccanismo aumenta la scarsità di Bitcoin, contribuendo potenzialmente a sostenerne il valore nel lungo periodo.
L’evento avviene automaticamente al raggiungimento del blocco numero 210 000, indipendentemente dal prezzo di mercato o dal tasso di hash della rete.

Al tempo della prima transazione nel 2009 e fino al 2012, il premio per ogni blocco risolto era di 50 bitcoin
Il 28 novembre 2012 si è verificato il primo halving, dimezzando le ricompense dei miner a 25 bitcoin.
Duecentodiecimila blocchi più tardi, il 9 luglio 2016, si è verificato un altro dimezzamento, portano la ricompensa a 12,5 bitcoin per blocco estratto

# Halving

Il terzo dimezzamento è avvenuto a Maggio 2020 quando è stato estratto il blocco numero 630.000. Il numero di bitcoin estraibili quotidianamente è passato da 1.800 a 900 al giorno. Ricompensa del blocco "= 6,25" bitcoin. La ricompensa verrà azzerata definitivamente nel 2140 quando il numero complessivo di bitcoin esistenti dovrebbe raggiungere 21 milioni

# Halving

Bitcoin ha completato con successo il suo quarto halving (20/04/2024), all'estrazione del blocco numero 840.000: da questo momento in avanti, i miner riceveranno metà delle ricompense. A partire dal 21/04, i miner di Bitcoin riceveranno 3, 125 BTC per ogni blocco estratto, rispetto ai precedenti 6, 25 BTC. Si tratta di un processo programmato nel protocollo di Bitcoin che avviene automaticamente ogni 210.000 blocchi minati, ovvero ogni circa ogni quattro anni.

# Validazione tramite mining

L’idea originale che ogni nodo possa concorrere alla validazione dei blocchi si è rivelata illusoria perché un utente con un singolo PC, anche molto potente, non ha alcuna possibilià di competere con centri dedicati che utilizzano ormai grandi sistemi paralleli composti di chip ASIC (application specific integrated circuit) per il calcolo super rapido della funzione SHA-256

# Validazione tramite mining

Per gestire l'ingombro crescente della blockchain, si adottano diverse tecniche che "tagliano" i rami più antichi senza spezzare la catena di hash

Una considerazione finale riguarda lo spazio nella memoria dei nodi che la sempre crescente block-chain invade progressivamente. A tale proposito vengono messi in atto vari accorgimenti per strutturare la catena nella forma di albero compatto in cui sia semplice eseguire ricerche di passate transazioni che possano mantenere interesse tagliando rami molto antichi senza interrompere la catena di hash

# Aspetti di sicurezza

La sicurezza di Bitcoin è basata sulla crittografia. Alcune sue caratteristiche specifiche potrebbero però renderlo attaccabile. Consideriamo anzitutto il cifrario asimmetrico impiegato per la costruzione degli indirizzi e per la firma delle transazioni. Mentre la crittografia su curve ellittiche risulta oggi sostanzialmente inattaccabile, l'importanza di proteggere e trattare le chiavi è più che mai cruciale in bitcoin

# Aspetti di sicurezza

Le chiavi pubbliche costituiscono di fatto gli indirizzi degli utenti; perciò in una transazione del tipo "$A$ paga $X$ bitcoin a $B$", l'utente $A$ deve accertarsi dell'indirizzo di $B$ per non dirigere il pagamento a qualcun altro senza possibilità di correzione successiva.

# Aspetti di sicurezza

Nel sistema bitcoin non esiste un ente tipo Certification Authority che garantisce l'autenticità delle chiavi. Né, per proteggere l'anonimato, esiste un registro pubblico che associa agli indirizzi bitcoin l'identità degli utenti. Questi potranno scambiarsi indirizzi bitcoin tra conoscenti come si fa per gli indirizzi e-mail, o più comunemente un esercizio commerciale potrà comunicare a un cliente il suo indirizzo per ricevere un pagamento, con tutti i problemi che possono presentarsi se ciò avviene in rete. Quanto alle chiavi private abbiamo già detto: la loro perdita comporta la perdita dei propri fondi, e il loro furto permette ad altri di utilizzarli senza possibilità di recupero. La firma delle transazioni non presenta invece problemi

# Aspetti di sicurezza

La mancanza di una certificazione esterna delle chiavi mostra anche che se il software di due utenti dovesse generare la stessa coppia di chiavi vi sarebbe inevitabilmente una commistione di fondi. Si può però dimostrare che questo evento ha una probabilità tanto piccola di verificarsi che gli utenti possono di fatto ignorare il problema. Inoltre questa remota eventualità può non essere troppo grave perché, per un motivo generale di protezione dei fondi, ogni utente è in genere invitato a crearsi diverse coppie di chiavi e quindi diversi indirizzi

# Aspetti di sicurezza

I problemi più seri sulle chiavi, come spesso avviene in crittografia, derivano da attacchi "laterali" che non sono diretti ai protocolli ma ai sistemi operativi dei calcolatori che li ospitano. L'installazione fraudolenta di malware in un PC può causare l'individuazione e il furto delle chiavi bitcoin al suo interno

# Aspetti di sicurezza

L'altra serie di attacchi, studiata sin dalla proposta iniziale di Nakamoto, consiste nell'intervenire sul mining per registrare transazioni false che accreditino fondi non dovuti, o cancellino pagamenti attraverso l'eliminazione di transizioni dai blocchi, o permettano di spendere più volte gli stessi fondi convalidando transazioni multiple. La difesa generale è insita nel criterio stesso di mining. Per avere una buona probabilità di convalidare falsamente un blocco un sistema deve avere una potenza di calcolo maggiore di quella del miner più potente: in questo caso potrebbe convenirgli di usare questa potenza per superare gli altri in un mining onesto guadagnando i bitcoin assegnati per questo lavoro

# Aspetti di sicurezza

Particolarmente serio sarebbe un intervento dell'attaccante che riguardi blocchi ormai convalidati e inseriti nella catena, per generare una catena diversa che si ponga in antitesi a quella corretta. Ma per modificare un blocco passato è necessario aggiornare anche tutti i successivi a causa della concatenazione di hash tra i blocchi della catena: ciò richiede di ricalcolare i nonce di tutti i blocchi interessati che è un lavoro computazionalmente enorme

# Aspetti di sicurezza

L’unica possibilià concreta di attacco sembrerebbe la scoperta di una falla nella funzione SHA-256 che permetta di prevederne in parte l’immagine prodotta rendendo più veloce la generazione dei nonce. Tale falla dovrebbe però essere scoperta e tenuta segreta dall’attaccante altrimenti tutti i miner potrebbero sfruttarla riportando la competizione al punto di partenza

# Anonimato

Un altro aspetto di bitcoin riguarda l'anonimato degli utenti. Poiché gli indirizzi non riportano dati che permettano di risalire a individui o organizzazioni particolari l'anonimato dovrebbe essere automaticamente garantito. Molti governi sono però intervenuti obbligando i sistemi che gestiscono il servizio a rilasciare informazioni sugli utenti, in particolare su coloro che acquistano o vendono bitcoin contro valute standard

# Implicazioni socioeconomiche

Dal 2009, anno della sua nascita, bitcoin è stato adottato da un numero sempre crescente di utenti ed è divenuto un'icona dei movimenti politici contrari allo strapotere dei governi e degli istituti finanziari

# Implicazioni socioeconomiche

I bitcoin sono creati e attribuiti come effetto della dimostrazione di aver eseguito un "duro lavoro" (il mining) che richiede grande dispendio di hardware e di energia elettrica. Quindi la creazione di bitcoin inquina l'ambiente; molto meno, però, dei sofisticati procedimenti per coniare monete e stampare banconote, e dei colossali sistemi di sicurezza per proteggerle e distribuirle. Come impatto sull'ambiente bitcoin batte le valute tradizionali senza possibilità di confronto

# Implicazioni socioeconomiche

Un altro aspetto rilevante è che bitcoin ha subito nella sua breve storia incredibili fluttuazioni di valore. Il fenomeno ha comunque generato una corsa all'acquisto di bitcoin come bene di investimento ad alto rischio consegnando capitali considerevoli nelle mani di semplici speculatori che non li hanno guadagnati con il loro lavoro (di mining). Con comprensibile irritazione dei suoi onesti sostenitori, la moneta elettronica non si è dunque ancora attestata come moneta "democratica", tale da recare giustizia sociale nell'economia

# Implicazioni socioeconomiche

Per comprendere meglio la portata del fenomeno è bene ricordare che il sistema prevede che i bitcoin possano essere scambiati liberamente con altre valute: il primo terminale ATM dove tali cambi possono aver luogo è stato installato in Canada nel 2013 e suoi simili si stanno lentamente diffondendo in altri paesi: primo tra tutti gli Stai Uniti dove bitcoin è stato sostanzialmente accettato nell'economia ufficiale (mentre in Cina è pesantemente osteggiato)

# Implicazioni socioeconomiche

Un campo in cui la moneta elettronica può intervenire per favorire l'equilibrio sociale è nelle rimesse di denaro che i migranti effettuano a vantaggio dei loro familiari in paesi lontani: rimesse al momento gestite da agenzie internazionali che si fanno pagare il servizio praticando in genere altissimi tassi di cambio

# Implicazioni socioeconomiche

Veniamo infine all'aspetto più largamente discusso di bitcoin che riguarda l'uso che se ne può fare. Bitcoin è stato purtroppo impiegato in pesanti operazioni illegali, scoperte e largamente rese note su Web, il che lascia prevedere che altre simili siano in atto o lo saranno in futuro. Si tratta di commercio di droga e di materiale pedopornografico, di riciclaggio di denaro sporco, tanto che la tendenza di tutti i governi è porre in opera misure di controllo che rischiano di limitare la libera circolazione della moneta elettronica